Nos. 25-1555 through 25-1578; 25-1580 through 25-1593; 25-1676; and 25-1677
(Consolidated)

IN THE UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

ATLAS DATA PRIVACY CORP., AS ASSIGNEE OF INDIVIDUALS WHO ARE COVERED PERSONS; JANE DOE 1, A LAW ENFORCEMENT OFFICER; JANE DOE 2, A LAW ENFORCEMENT OFFICER; EDWIN MALDONADO; SCOTT MALONEY; JUSTYNA MALONEY; PATRICK COLLIGAN; PETER ANDREYEV; AND WILLIAM SULLIVAN,

PLAINTIFFS-APPELLEES,

v.

WE INFORM LLC, ET AL.,

DEFENDANTS-APPELLANTS.

On Appeal from the Order and Memorandum of the United States District Court for the District of New Jersey dated November 26, 2024

APPELLEES' JOINT RESPONSE BRIEF

PEM LAW LLP
Rajiv D. Parikh, Esq.
Kathleen Barnett Einhorn, Esq.
Jessica A. Merejo, Esq.
One Boland Drive, Suite 101
West Orange, New Jersey 07052
Telephone: (973) 577-5500
rparikh@pemlawfirm.com
keinhorn@pemlawfirm.com
jmerejo@pemlawfirm.com

BOIES SCHILLER FLEXNER LLP
David Boies, Esq.
55 Hudson Yards, 20th Floor
New York, New York 10001
Telephone: (919) 749-8200
Email: dboies@bsfllp.com

Eric M. Palmer, Esq.
401 E. Las Olas Blvd., Suite 1200
Fort Lauderdale, Florida 33301
Telephone: (954) 377-4250
Email: epalmer@bsfllp.com

Mark C. Mao, Esq.
44 Montgomery Street, 41st Floor
San Francisco, California 94104
Telephone: (415) 293-6800
Email: mmao@bsfllp.com

Adam R. Shaw, Esq.
30 South Pearl Street, 12th Floor
Albany, New York 12207
Telephone: (518) 434-0600
Email: ashaw@bsfllp.com

MORGAN & MORGAN, P.A.
Ryan J. McGee, Esq.
John A. Yanchunis, Esq.
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Emails: rmcgee@forthepeople.com
jyanchunis@forthepeople.com

BIRD MARELLA RHOW LINCENBERG DROOKS NESSIM LLP
Ekwan E. Rhow, Esq.
Elliot C. Harvey Schatmeier, Esq.

Bill L. Clawges, Esq.
1875 Century Park East, 23rd Fl
Los Angeles, California 90067
Telephone: (310) 201-2100
Emails: erhow@birdmarella.com
ehs@birdmarella.com
bclawges@birdmarella.com

Attorneys for Appellees

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, Plaintiff-Appellee Atlas Data Privacy Corporation hereby states that it does not have any parent companies and no publicly held corporation owns 10% or more of such company's stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTRODUCTION

In July 2020, an attorney attacked the family of Judge Esther Salas at their New Jersey home, killing her son Daniel Anderl, who was celebrating his twentieth birthday, and leaving her husband Mark Anderl in critical condition from multiple gunshot wounds. The murderer, who had intended to kill Judge Salas, obtained her home address from data brokers that made it readily available online. In response to this tragedy, the New Jersey Legislature unanimously enacted Daniel's Law, which provides New Jersey judges, prosecutors, law-enforcement officers, and their immediate family members (collectively "covered persons") with multiple mechanisms "to enhance" their own "safety and security" and "carry out their official duties without fear of personal reprisal." N.J.S.A. 56:8-166.3.[1]

Daniel's Law provides "covered persons" with a civil cause of action against private entities who continue to disclose, re-disclose, or otherwise make available their home addresses or unpublished telephone numbers more than ten business days after receiving a nondisclosure request from that covered person. *Id.* 56:8-166.1(d). The law, as amended, also created a new administrative agency, the Office of Information Privacy (OIP), to enable covered persons to redact their protected information from New Jersey public records. The public-records redaction system

[1] All relevant Complaints are materially the same for purposes of this Brief. All internal quotation marks and citations are omitted unless otherwise indicated.

created by the statute is so comprehensive that covered persons can redact their addresses from deeds, leases, mortgages. N.J.S.A. 46:26A-2.

Plaintiffs-Appellees filed these cases after Defendants persisted in disclosing the addresses and/or phone numbers of some 19,000 covered persons despite receiving written requests from them to cease such disclosure. Today, nearly one-and-half years after receiving those thousands of nondisclosure requests, many Defendants continue to not comply with their obligations under Daniel's Law. Plaintiffs filed these suits in New Jersey Superior Courts. After removing these cases to federal court—and requesting that every Judge in the District of New Jersey recuse themselves—Defendants decided to argue that the law is facially unconstitutional under the First and Fourteenth Amendments, while many remain out of compliance.

To establish their facial challenge, Defendants needed to show that "a substantial number of [the law's] applications are unconstitutional, judged in relation to the statute's plainly legitimate sweep." *Moody v. NetChoice, LLC*, 603 U.S. 707, 723 (2024). Even under the more forgiving standard applied in the First Amendment context, "[a] law with a plainly legitimate sweep may be struck down in its entirety…only if the law's unconstitutional applications substantially outweigh its constitutional ones." *Id.* at 723-34. And Defendants had "burden on those issues as the price of [their] decision to challenge the law[] as a whole." *Id*.

Unsurprisingly, Defendants failed to meet this burden. Defendants' facial challenge was governed by the test articulated in *Florida Star v. B.J.F.*, 491 U.S. 524 (1989), and *Smith v. Daily Mail Publishing Co.*, 443 U.S. 97 (1979)—which is known as "the *Daily Mail* test." *Schrader v. District Att'y of York Cnty.*, 74 F.4th 120, 127–28 (3d Cir. 2023). Under that test, a constitutional challenge to a state privacy tort can succeed only if two requirements are met. "The first inquiry" is whether the speaker disclosed "'lawfully obtain[ed], truthful information about a matter of public significance.'" *Florida Star*, 491 U.S. at 536 (quoting *Daily Mail*, 443 U.S. at 103). If the answer is "yes," "[t]he second inquiry is whether imposing liability" would "further a state interest of the highest order.'" *Id.* at 537 (quoting *Daily Mail*, 443 U.S. at 103).

But if the answer is "no," the defendant's challenge "fails the threshold test," and further "balancing does not come into play." *City of San Diego v. Roe*, 543 U.S. 77, 84 (2004) (applying "the same standard used to determine whether a common-law action for invasion of privacy is present"). The plaintiff's privacy interest outweighs the defendant's speech interest, and the defendants are not "entitled to 'special protection' under the First Amendment" from "tort liability." *Snyder v. Phelps*, 562 U.S. 443, 459 (2011).

As the District Court ruled, Defendants' attack on Daniel's Law failed at both stages of this inquiry. At the threshold step, Daniel's Law does not regulate speech

on a matter of public concern in the overwhelming majority of its applications—and at minimum, Defendants had no way of showing otherwise given their choice to raise this facial attack in a motion-to-dismiss stage. The District Court could have ended its analysis there, because Daniel's Law cannot be facially unconstitutional if it does not even regulate speech on a matter of public concern in a substantial number of applications.

Even at the second stage of the test, the statute is structured to include precisely the "more careful and inclusive precautions against alternative forms of dissemination" called for in *Florida Star*. 491 U.S. at 541. Indeed, the law is so well-tailored that Defendants ultimately could not come up with a single gap in OIP's record-redaction system. For these reasons, this Court should affirm.

BACKGROUND

I. Daniel's Law

Although Defendants refer to Daniel's Law as if it were a totality, the statute consists of multiple components. The first, entitled "Internet disclosure of certain information related to covered persons; civil liability," provides covered persons with a civil claim against any "person, business or association" who continues to disclose home addresses or unpublished telephone numbers more than ten business

days after receiving a nondisclosure request.[2] The second part relates to New Jersey's public-records law and creates OIP, a new administrative agency tasked with overseeing the redaction of the same information from virtually all public records. Another component, which is less relevant here, creates a criminal offense for "publishing" or "posting" a covered person's protected information "knowingly, with purpose to expose another to harassment or risk of harm to life or property, or in reckless disregard of the probability of such exposure." N.J.S.A. 2C:20-31.1(b).

A. The Private Cause of Action against Private Data Brokers for Private Data Records

Daniel's Law gives covered persons a right to request that a "person, business, or association" not "disclose or re-disclose on the Internet or otherwise make available" their "home address or unpublished home telephone number." *Id.* 56:8-166.1(a)(1), (d). To trigger one's rights under the statute, one needs to make a written request, and the statute provides recipients with time for compliance. The request must come from an "authorized person"—either a covered person or a designee—and must give the recipient of the request "written notice" that the requestor "is an authorized person." *Id.* 56:8-166.1(a)(2). And the recipient has "10 business days following receipt" before the duty to "not disclose or re-disclose" is imposed. *Id.*

[2] The statute defines "covered person" to refer to "an active, formerly active, or retired judicial officer, law enforcement officer, or child protective investigator . . . , or prosecutor and any immediate family member residing in the same household as such [individual]." N.J.S.A. § 56:8-166.1(d).

56:8-166.1(a)(1).[3] The statute does not prohibit dissemination of a covered person's protected information as a categorical rule. It only requires nondisclosure when a valid request is received, and a claim only arises after the recipient fails to comply with that request within ten business days.

A recipient who discloses the covered person's protected information after the ten-day period is liable for "actual damages, but not less than liquidated damages computed at the rate of $1,000 for each violation." *Id.* 56:8-166.1(c)(1). Punitive damages are available "upon proof of willful or reckless disregard." *Id.* 56:8-166.1(c)(2). Courts may also award "any other preliminary and equitable relief." *Id.* 56:8-166.1(c)(4). And to avoid obvious obstacles to effective enforcement against companies that routinely post or sell information on the Internet, the Legislature grants covered persons a statutory right to assign, "in writing," their "right to bring a civil action in response to a violation." *Id.* 56:8-166.1(b) & (d).

B. OIP's Public Records Redaction Process

Daniel's Law also provides a mechanism for covered persons to achieve redaction of their home addresses from New Jersey State and local public records. Covered persons can submit (or revoke) requests for redaction through a "secure

[3] The statute defines "disclose" to mean "solicit, sell, manufacture, give, provide, lend, trade, mail, deliver, transfer, post, publish, distribute, circulate, disseminate, present, exhibit, advertise, or offer" and includes "making available or viewable within a searchable list or database, regardless of whether a search of such list or database is actually performed." N.J.S.A. § 56:8-166.1d.

portal" created by OIP. N.J.S.A. 47:1B-1(c)(1). When a covered person's request for redaction is approved by OIP, public agencies "shall redact or cease to disclose" that person's address within 30 calendar days. *Id.* 47:1B-2(b).[4] The statute creates two regimes that allow highly limited disclosures of unredacted copies of (i) voter records and (ii) property records. Apart from that, the statute permits redaction of home addresses from virtually every category of public record maintained by State or local public entities in New Jersey.

Voter Records. Voter-registration files in the Statewide system or maintained by a county may be provided unredacted for the limited use in connection with election challenges, but only to an election challenger by a county or municipal party chair, to a candidate who appointed that challenger, or to a candidate acting as a challenger, and if and only if such individual signs an affidavit attesting to their qualifying status and to the limited use of the unredacted records. *Id.* 47:1B-3.1(a)-(c). A public agency may also share unredacted information with a "vendor, contractor, or organization carrying out a function of a county or of the State concerning the administration or conduct of elections," but the vendor or contractor

[4] OIP's process does not provide for redaction of phone numbers because any personal phone number that appears in public records is deemed confidential as a matter of law and expressly removed from the definition of a "Government Record" that could be subject to disclosure. N.J.S.A. § 47:1A-1.

is prohibited from using "such information in any manner other than as necessary to carry out the purposes of the agreement. *Id.* 47:1B-3.5.

Real Property Records. Daniel's Law allows covered persons to redact their address from any "document affecting the title to real property" that is "recorded and indexed by a county recording officer" or "otherwise held or maintained by" State and local tax officials. N.J.S.A. 47:1B-3a(2). N.J.S.A. 46:26A-2 defines "document affecting real property" to include all property interests "entitled to recording" under state law, which includes seventeen categories such as mortgages, deeds, and leases.[5] Subject to the three limited exceptions described below, for these records, the statute allows recordkeepers to redact "the names or other information" of covered persons

[5] Those categories are: (1) deeds or other conveyances, releases, or declarations of trust; (2) powers of attorney; (3) leases, or memoranda of leases, for life or a term not less than two years; (4) mortgages or other conveyances in the nature of a mortgage; (5) liens or encumbrances and releases of liens or encumbrances on any interest; (6) assignments, discharges, cancellations, or releases; (7) options and rights of first refusal; (8) certified copies of judgments, decrees and orders of courts of record; (9) reports of condemnation and declarations of taking; (10) restrictions affecting real property or its use; (11) notices of federal tax liens; (12) notices of settlement; (13) maps; (14) condominium master and unit deeds; (15) cooperative master declarations and proprietary leases; (16) any other document that affects title to any interest in real property in any way or contains any agreement in relation to real property, or grants any right or interest in real property or grants any lien on real property; and (17) any other document relating to real property that is directed to be recorded by any statute or court order. N.J.S.A. § 46:26A-2(a)-(q).

"instead of" or "in addition" to redacting their address as an alternative method of complying with the statute. *Id.* 47:1B-3a(2).

First, "document[s] affecting the title to real property" as defined by N.J.S.A. 46:26A-2, such as mortgages and deeds, may be provided unredacted but only to certain real-estate professionals licensed by the State when required in the ordinary course of business. These professionals are (a) title insurers; (b) mortgage insurers; (c) mortgage originators; (d) registered title-search businesses; and (e) real-estate brokers. *Id.* 47:1B-3(a)(2)(a)-(e). Unredacted property records may also be disclosed to a person engaged in a real-estate transaction with a covered person. *Id.* 47:1B-3(a)(2)(f).

Second, the statute wholly exempts from redaction "records evidencing any lien, judgment, or other encumbrance on real or other property". *Id.* 47:1B-3(a)(4)(d). But the scope of this exemption is extremely limited. Of the seventeen categories of "documents affecting real property" identified by N.J.S.A. 46:26A-2, this exemption applies to only two of them: "liens or encumbrances and releases of liens or encumbrances on any interest and judgments," and "certified copies of judgments, decrees and orders of courts of record." *Id.* 46:26A-2.

Third, assessment lists and each county's index of recorded documents may be viewed unredacted, but "only when inspected in person." *Id.* 47:1B-3(a)(4)(e) & (f). And when a document is "only available to be viewed in person," the statute

requires the "custodian or other government official" responsible for the document to "make every reasonable effort to hide such address when allowing an individual without authority to view such address as unredacted to view the record." *Id.* 47:1B-3(a)(6).

Other Exceptions. Apart from these limited-access regimes governing voter records and property records, agencies may provide unredacted records in only a handful of highly limited circumstances. A public agency may share unredacted information with a "vendor, contractor, or organization" but the vendor or contractor is prohibiting from using "such information in any manner other than as necessary to carry out the purposes of the agreement." *Id.* 47:1B-3(a)(5). Similarly, an agency may provide home addresses (but not telephone numbers) to the majority representative of its employees. *Id.* 47:1B-3(a)(3). Covered persons also cannot redact their addresses from Uniform Commercial Code filings and financing statements; petitions naming candidates for office (where the covered person themselves is a candidate); voter petitions (that the covered person signed); and records concerning property presumed abandoned under New Jersey's Uniform Unclaimed Property Act. *Id.* 47:1B-3(a)(4)(a)-(c) & (g). And information otherwise subject to redaction "may be provided as unredacted upon order of a judge" of any "court of competent jurisdiction." *Id.* 47:1B-3(c).

II. Facts And Procedural History

A. These Cases

Plaintiffs in these cases are Atlas Data Privacy Corporation ("Atlas"), Jane Doe-1, Jane Doe-2, Edwin Maldonado, Scott Maloney, Justyna Maloney, Patrick Colligan, Peter Andreyev, and William Sullivan. JA487–90. Atlas is the assignee of over 19,000 covered persons who used Atlas's platform to send Defendants written notices to cease disclosure of their protected information and then, after their requests were not complied with, assigned their claims to Atlas to pursue in court. JA541.[6] The named individual plaintiffs are police officers or correctional officers who are covered persons under Daniel's Law. JA487–91. Defendants include data brokers, real estate businesses, and direct-mailing/ marketing companies. Appellants' Br. at 15–16.

Each of the individual plaintiffs, as well as many other prosecutors and law-enforcement officers who assigned their claims to Atlas in these cases, have faced

[6] Atlas owns and operates an online platform, including an email service named AtlasMail, for covered persons to identify data brokers and send written nondisclosure notices. Upon signing up for the Atlas platform, a covered person is asked a series of questions to collect protected information and qualify their eligibility under Daniel's Law. The covered person receives their own AtlasMail account with a unique inbox address (e.g. john.doe23@atlasmail.com). Atlas provides recommended lists of data brokers involved in the disclosure in protected information, and a covered person can choose to send nondisclosure requests to some or all of these brokers via their AtlasMail address, or skip the sending process altogether and defer that choice to a later date.

harassment and threats to their lives and the lives of their family members as a result of their public service. JA487–91.

Beginning in February 2024, Plaintiffs filed these actions in Superior Court in several counties in New Jersey. JA091. The eight individual Plaintiffs, six police officers and two correctional officers, allege that they were threatened with violence as a result of their public service. JA487–91. After Daniel's Law was enacted, each individual Plaintiff sent Defendants written notices requesting that Defendants cease disclosing or re-disclosing their home address and unpublished telephone number. JA491. Most Defendants never responded to the written notices, and all Defendants continued to disclose the protected information of the individual Plaintiffs or the other 19,000 covered persons who assigned their claims to Atlas. JA100; JA491. Many Defendants are still not compliant with the law. *E.g.*, JA491.

Defendants removed the actions to the United States District Court for the District of New Jersey, and sought recusal of all of the judges of that District. JA091. On April 2, 2024, this Court reassigned these actions to District Judge Harvey Bartle III pursuant to 28 U.S.C. § 292(b). *Id.* The District Court stayed all actions except for motions to dismiss on the ground of facial unconstitutionality and further challenges to subject-matter jurisdiction for the removal. JA092.

On June 10, 2024, Defendants moved to dismiss the complaints, arguing that Daniel's Law is unconstitutional on its face under the First Amendment. *Id.* The

District Court gave notice to the Attorney General of New Jersey, who intervened to defend the law. *Id.* The District Court subsequently remanded 39 of the cases for lack of diversity jurisdiction. *Id.*

B. The District Court's Order

On November 26, 2024, the District Court denied Defendants' motion to dismiss. The District Court concluded that Defendants' facial challenge was governed by the *Daily Mail* test because Daniel's Law is "part of the long history of common law torts and statutes whose purpose is to afford redress to persons whose privacy is invaded from disclosure of personal information, albeit truthful, that is not of public interest." JA105. At the first step of the test, the District Court concluded that, in general, "home addresses and unpublished telephone numbers are not matters of public significance," while leaving room for as-applied challenges in future "hypotheticals" in which the protected information "of a covered person may be newsworthy." JA109–10. As noted, the District Court could have ended its analysis there, because the *Daily Mail* test does not mandate further scrutiny of speech that fails the threshold "public concern" test.

But the District Court proceeded to the second step of the test and found that that Daniel's Law is narrowly tailored "to further a state interest of the highest order." JA110–11. The District Court found it to be a "well-known fact, amply documented by the record here, that in recent years judges, prosecutors, police, correctional

officers, and others in law-enforcement have been the subject of an ever increasing number of threats and assassinations." JA110. The District Court further found that "[s]ome of these threats and assassinations, as alleged in the complaints and of which the court takes judicial notice, have been facilitated by malefactors obtaining the home address or unlisted phone number of their targets." *Id.* The District Court also ruled that interpreting the statute to adopt "a negligence standard" is "a reasonable construction of Daniel's Law, avoids absurd results, is consistent with analogous New Jersey privacy law, and saves the law from constitutional repugnancy." JA120.

On December 2, 2024, the District Court certified its order under 28 U.S.C. § 1292(b). JA131. Defendants filed a Petition seeking interlocutory review, which this Court granted on March 18, 2025. JA014.

STANDARD OF REVIEW

This Court reviews a ruling on a motion to dismiss *de novo*, and "may affirm on any ground supported by the record." *Wilson v. USI Ins. Serv. LLC*, 57 F.4th 131, 139-40 (3d Cir. 2023).

SUMMARY

I. Defendants' facial challenge clearly fails under the *Daily Mail* test. Contrary to Defendants' arguments, this Court and the Supreme Court have applied the *Daily Mail* to statutes that create privacy torts, regardless of whether the "restriction on speech [was] content-based." *Schrader*, 74 F.4th at 126. That test applies here

because the disclosures regulated by Daniel's Law "implicate[] plaintiffs' privacy interests by disclosing their home addresses" and undermining their ability to "list their telephones privately." *Paul P. v. Verniero*, 170 F.7d 396, 404 & 406 (3d Cir. 1999) ("*Paul P. I*") (interest in non-disclosure of one's address is shielded by the "constitutional right to privacy"). Under the *Daily Mail* test, Defendants' facial challenge "fails the threshold test," because the overwhelming majority of the disclosures regulated by Daniel's Law have nothing to do with any matter of "legitimate news interest." *Roe*, 543 U.S. at 84.

II. If this Court nonetheless subjects Daniel's Law to review under the tiers of scrutiny, it should apply intermediate scrutiny. First, Daniel's Law is not content-based because addresses and phone numbers do not in themselves qualify as "content," and the statute does not "target" that data by reference to any message of the speaker. *Project Veritas v. Schmidt*, 125 F.4th 929, 961 (9th Cir. 2025). Second, Daniel's Law belongs to a family of common-law and statutory disclosure of private facts torts of "longstanding coexistence with the First Amendment." *Vidal v. Elster*, 602 U.S. 286, 300 (2024). And third, any risk of viewpoint discrimination is trivial, so "intermediate scrutiny" can apply to the statute even "without any reliance on history." *VoteAmerica v. Schwab*, 121 F.4th 822, 849 (10th Cir. 2024).

III. Daniel's Law survives facial scrutiny under any standard, including strict scrutiny, because it is narrowly tailored to advance a compelling state interest.

Defendants argue that the statute's definition of "disclose" is overbroad, but their examples of supposedly innocuous disclosures of covered persons' protected information illustrate why the statute needed to include "alternative forms of dissemination" rather than imposing the "selective ban on publication by mass media" advocated by Defendants. *Florida Star*, 491 U.S. at 541. Most obviously, if "*providing*" an address to a law firm were exempted from the statute, Daniel's Law could not even have prevented the very murder that led to its enactment, because it was an attorney who targeted Judge Salas and murdered her son. Defendants' argument that Daniel's Law is somehow both over- and underinclusive because it does not enable covered persons to redact their addresses from every public record maintained by the State grossly understates the redaction available under the statute and overlooks phone numbers entirely.

Apart from that, Defendants offer nothing more than a series of complaints about the absence of a "verification" provision in Daniel's Law, and its authorization of assignment and liquidated damages. None of these arguments are even relevant to the First Amendment inquiry, because these provisions have nothing to do with how much protected speech the statute restricts. Thus, even under strict scrutiny, this Court can easily affirm the District Court's ruling.

ARGUMENT

I. Daniel's Law Is Facially Constitutional Under the Supreme Court's Privacy Precedents

A. The *Daily Mail* Test Applies to Torts That Protect Privacy, Regardless of Whether They Are Content-Based

Defendants' lead challenge contends (at 42) that "[c]ontent-based laws" are categorically "subject to strict scrutiny even when they implicate privacy interests." But as this Court has explained, the Supreme Court has applied the *Daily Mail* test to statutes regardless of whether the "restriction on speech [was] content-based," and that test "stands apart from the content-focused analysis." *Schrader*, 74 F.4th at 126 & 128. *Florida Star* applied that test to a statute that imposed tort liability on publications of "the ***name, address, or other identifying fact or information***" of the "victim of any sexual offense," 491 U.S. at 526 n.1 (emphasis added) (quoting Fla. Stat. § 794.03 (1987)).[7] *Daily Mail* applied the test to a statute prohibiting disclosure of "the name of any child" involved in "a juvenile proceeding." 443 U.S. at 99. And *Cox Broadcasting Corp. v. Cohn*, recognized that the common-law "cause of action

[7] Neither *Reed v. Town of Gilbert*, 576 U.S. 155 (2015), nor *Barr v. American Association of Political Consultants, Inc.*, 591 U.S. 610 (2020), addressed the *Daily Mail* test, and the Supreme Court "does not normally overturn, or so dramatically limit, earlier authority *sub silentio*," *Shalala v. Illinois Council on Long Term Care, Inc.*, 529 U.S. 1, 18 (2000). Although *Barr* upheld the Telephone Consumer Protection Act under strict scrutiny, that statute regulates robocalls, not disclosures of private information, so the *Daily Mail* test did not apply.

for invasion of privacy through public disclosure" imposes sanctions on "content." 420 U.S. 469, 495 (1975).

This Court and other Circuits have applied the *Daily Mail* test to statutes that must be content based if Daniel's Law is. In *Bowley v. City of Uniontown Police Dept't*, this Court applied *Daily Mail* to a statute prohibiting disclosure of "[t]he ***contents*** of law enforcement records…concerning a child." 404 F.3d 783, 786 & n.3 (3d Cir. 2005) (quoting 42 Pa. Cons. Stat. § 6308)). In Defendants' own case, the Fourth Circuit held that a statute prohibiting disclosure of Social Security Numbers "must be evaluated using the *Daily Mail* standard." *Ostergren v. Cuccinelli*, 615 F.3d 263, 276 (4th Cir. 2010); *see also Peavy v. WFAA-TV, Inc.*, 221 F.3d 158, 189 (5th Cir. 2000) ("[T]he Court did *not* rely on the content-based nature of the statutes" in *Florida Star* or *Daily Mail*).

Defendants misunderstand *Schrader* when they claim (at 42–43) it "addressed the relationship between the content-based restriction test and the *Daily Mail* test" and held that statutes like Daniel's Law "must survive *both* tests." *Schrader* declined to decide whether to apply the tiers of scrutiny or *Daily Mail* to a statute because both tests "point[ed] the same way" on the facts. 74 F.4th at 126. [8] *Schrader* never suggested privacy statutes *must* satisfy both tests—as if statutes that protect privacy

[8] The Court could do the same here, because Daniel's Law survives even strict scrutiny, *infra* 37-54.

were somehow subject to a *more demanding* standard than strict scrutiny despite Supreme Court's repeated insistence "on limited principles that sweep no more broadly than the appropriate context of the instant case" in cases dealing with "clashes between [the] First Amendment and privacy rights." *Bartnicki v. Vopper*, 532 U.S. 514, 529 (2001).

The closest Defendants come to a case at odds with *Daily Mail* is *IMDb.com Inc. v. Becerra*, 962 F.3d 1111 (9th Cir. 2020), where the Ninth Circuit applied strict scrutiny to a statute that required "commercial online entertainment service provider[s]" to remove actors' and other entertainers' ages and dates of birth from profiles created by members of the public on IMDb's website. *Id.* at 1117-18. But the Ninth Circuit did not appear to appreciate that the *Daily Mail* test has been applied to both content-based and content-neutral statutes and materially differs from strict scrutiny in its focus on whether the speech at issue is of public concern. At any rate, *IMDb* is distinguishable, because the Ninth Circuit likely could have applied strict scrutiny there anyways. It is unclear whether the statute there would trigger the *Daily Mail* test, because disclosing someone's "date of birth" ordinarily "does not implicate a privacy interest." *Paul P. v. Farmer*, 227 F.3d 98, 106 (3d Cir. 2000) ("*Paul P. II*"). Beyond that, the statute compelled "a single category of speakers" to exercise their editorial discretion over content submitted by third parties

that potentially implicated compelled-speech and speaker-targeting concerns absent from these cases. *IMDb*, 962 F.3d at 1120.

Defendants also suggest that applying *Daily Mail* here would recognize a "new category" of unprotected speech, in contravention of *Brown v. Entertainment Merchants Association*, 564 U.S. 786 (2011). But the *Daily Mail* test is neither "new" nor a category of "unprotected speech." The test has existed since the Supreme Court decided *Daily Mail* and has applied to statutes like Daniel's Law since *Florida Star*. And under the test, "speech, even if not touching upon a matter of public concern," is not "totally beyond the protection of the First Amendment." *Connick v. Myers*, 461 U.S. 138, 148 (1983). Such speech cannot be regulated under the *Daily Mail* standard for a purpose other than imposing tort liability. *See Ostergren*, 615 F.3d at 271-74 (distinguishing whether disclosures are "unprotected speech" under *Brown* from whether the *Daily Mail* test applies).

There is nothing unusual about this framework. In many areas where "free expression necessarily conflicts with other protected rights," courts "balance the interests underlying the right to free expression against the interests in protecting the right" of the other party rather than applying the generic tiers of scrutiny. *Hart v. Electronic Arts, Inc.*, 717 F.3d 141, 149 (3d Cir. 2013) (right of publicity); *Snyder*, 562 U.S. at 451 (2011) (IIED); *New York Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964) (defamation); *Time, Inc. v. Hill*, 385 U.S. 374 (1967) (false light). Generally,

when the First Amendment "serve[s] as a defense in state tort suits," the inquiry "turns largely on whether that speech is of public or private concern, as determined by all the circumstances of the case." *Snyder*, 562 U.S. at 451. As in other areas, "further First Amendment scrutiny is unnecessary" apart from the application of this "built-in free speech safeguard[]." *Eldred v. Ashcroft*, 537 U.S. 186, 221 (2003) (copyright); *Vidal*, 602 U.S. at 300 (trademark).

B. The *Daily Mail* Test Is Grounded In The Original Meaning Of The First Amendment

If the Court feels the need to reexamine the history of the *Daily Mail* test, however, that test is fully consistent with the original meaning of the First Amendment and has a stronger grounding in common-law tradition than the tiers of scrutiny. "From the Founding through the early twentieth century," states had broad power to "restrict expression to promote the public good subject to the rule against prior restraints and the privilege of discussing matters of public concern in good faith." J. Campbell, *The Emergence of Neutrality*, 131 Yale L.J. 861, 870 (2022). Courts only began to "treat speech and press rights as nondiscrimination rules that made content-based restrictions presumptively unconstitutional" in the twentieth century. *Id.* Before then, the constitutional protection in tort cases was that "[s]peech on matters of public concern was privileged" unless it "aimed at undermining the public good." *Id.* at 887. This approach was based on the original understanding of speech and press freedoms as "natural rights" that were "subject to restrictions under

laws that promoted the public good" and that prevented interference "with the rights of others." J. Campbell, *Natural Rights and the First Amendment*, 127 Yale L.J. 246, 276-77 (2017). But because "the Founders recognized considerable underdeterminacy about what natural law required," courts relied on "the common law" to "determine the proper boundaries of natural liberty." *Id.* at 291.

The foundational common-law privacy cases applied the same understanding of speech to privacy torts, recognizing that "[t]he right of privacy is unquestionably limited by the right to speak and print" on "matters of a public nature." *Pavesich v. New England* Life Ins. Co., 50 S.E. 68, 74 (Ga. 1905); *Melvin v. Reid*, 297 P. 91, 92 (Cal. Ct. App. 1931); S. Warren & L. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 214 (1890) ("The right to privacy does not prohibit any publication of matter which is of public or general interest.").[9] Courts identified speech and privacy as "natural right[s]" that must be "enforced with due respect for the other." and adopted the public-concern standard precisely because of its grounding in "the common law rules which were in force when the constitutional guarantees were adopted."

[9] The contemporary privacy torts were developed after the rise of mass media in the late 19th century. But "Warren and Brandeis did not invent the right to privacy . . . . By 1890, a robust body of confidentiality law protecting private information from disclosure existed throughout…common law." N. Richards & D. Solove, *Privacy's Other Path*, 96 Geo. L.J. 123, 125 (2007); *see also* E. Bloustein, *Privacy as an Aspect of Human Dignity*, 39 N.Y.U. L. Rev. 962 (1964) (cited by *Cox Broadcasting*, 420 U.S. at 487 n.15).

Pavesich, 50 S.E. at 73; *see also McGovern v. Van Riper*, 43 A.2d 514 (N.J. Ch. 1945) ("[T]he right of privacy ha[s] its origin in natural law.").

Thus, well before *Daily Mail*, courts had a settled framework for managing conflicts between speech and privacy that was "plainly rooted in the traditions and significant concerns of our society." *Cox Broadcasting,* 420 U.S. at 491 & 493 (recognizing a "privilege in the press to report the events of judicial proceedings"). *Cox Broadcasting* and *Florida Star* constitutionalized that framework. *See Anderson v. Suiters*, 499 F.3d 1228, 1236 (10th Cir. 2007) ("[L]egitimate public concern is both an element of the common law tort and a constitutional limitation imposed by the First Amendment."). A test with such a "longstanding coexistence…with the First Amendment" cannot be doubted. *Vidal*, 602 U.S. at 288.

C. Daniel's Law Protects Compelling Privacy Interests

Apart from their attack on the *Daily Mail* test, Defendants contend (at 44-45) that Daniel's Law "is not a 'privacy law'" to which that test would apply. But Daniel's Law protects the "interest in one's home address by all persons who do not wish it disclosed," which this Court has long held to be a privacy interest of constitutional magnitude. *Paul P. I*, 170 F.3d at 404 ("[H]ome addresses are entitled to some privacy protection, whether or not so required by a statute."); *Paul P. II*, 227 F.3d at 106-107 (same); *A.A. ex rel M.M. v. New Jersey*, 341 F.3d 206, 214 (3d Cir.

2003) (same); *Kallstrom v. City of Columbus*, 136 F.3d 1055, 1064 (6th Cir. 1998) (addresses and phone numbers).[10]

For covered persons, this privacy interest is far stronger. For them, "disclosure of this protected information" creates "a very real threat to the officers' and their family members' personal security and bodily integrity, and possibly their lives." *Kallstrom*, 136 F.3d at 1064 (holding "release of private information concerning the officers…rises to constitutional dimensions by threatening the personal security and bodily integrity of the officers and their family members"). And if a privacy interest is sufficiently well-entrenched to be recognized as a "fundamental" incident of the "right to be let alone" protected by the Fifth and Fourteenth Amendments, that interest is clearly one states are entitled to protect through tort law. *Westinghouse*, 638 F.2d at 576. "Both the rights of freedom of speech" and "the right to privacy" are "fundamental constitutional rights," so "courts are required to engage in a fact-sensitive balancing, with an eye toward that which is reasonable and that which resonates with our community morals." *Toffoloni v. LFP Publ'g Grp.*, 572 F.3d 1201, 1212 (11th Cir. 2009).

[10] Defendants mischaracterize *Paul P. II* (at 46) as a FOIA case, even though it recognized this privacy interest "as a matter of federal constitutional law." 227 F.3d at 107. And although constitutional rights run against governments, caselaw has never drawn a firm distinction between privacy rights against the government and privacy rights against private parties, grounding both in the general "right to be let alone." *United States v. Westinghouse*, 638 F.2d 570, 576 (3d Cir. 1980).

Defendants' attempts to show Daniel's Law does not protect privacy are meritless. First, Defendants note (at 44) that the text of Daniel's Law references "safety and security," not privacy. N.J.S.A. 56:8-166.3. But the text of Daniel's Law identifies two aims—"safety" and "security"—and "each" of those words must be "give[n] [a] meaning" of its own. *Patel v. New Jersey Motor Vehicle Comm'n*, 982 A.2d 445, 425 (N.J. 2009). If "safety" refers to physical safety, the term "security" naturally encompasses "the security of one's privacy." *Sterling v. Borough of Minersville*, 232 F.3d 190, 197 (3d Cir. 2000); *Westinghouse*, 638 F.2d at 580 (privacy encompasses the "security" of "information against subsequent unauthorized disclosure.").

Second, Defendants assert that addresses and phone numbers inherently constitute "public fact[s]," the disclosure of which "cannot be viewed as an invasion of privacy." *McNutt v. New Mexico State Tribune Co.*, 538 P.2d 804, 808 (N.M. Ct. App. 1975). But this argument assumes a "secrecy" conception of privacy, in which there is "no remedy where the disclosed information was already publicly available." *Ostergren*, 615 F.3d at 283. The privacy interest protected by Daniel's Law is not based on secrecy, but "instead involves 'the individual's control of information concerning his or her person,'" which can be "misused repeatedly" if it is freely disclosed in an unauthorized manner. *Id.* at 282-83 (quoting *U.S. Dep't of Def. v. FLRA*, 510 U.S. 487, 500 (1994)).

An "interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form." *FLRA*, 510 U.S. at 500. Nor does it "'fade when the information involved already appears on the public record.'" *Ostergren*, 615 F.3d at 283 (quoting *Cox Broadcasting*, 420 U.S. at 494-95). Thus, as this Court has held, "[t]he compilation of home addresses in *widely available* telephone directories" does not show "addresses are not considered private." *Paul P. I*, 170 F.3d at 404 (emphasis added); *see also FLRA*, 510 U.S. at 501 ("[H]ome addresses are often publicly available through sources such as telephone directories and voter registration lists, but '[i]n an organized society, there are few facts that are not at one time or another divulged.'" (quoting *U.S. Dep't of Just. v. Reps. Comm. For Freedom of Press*, 489 U.S. 749, 763 (1989)("*RCFP*")).[11]

Third, Defendants claim (at 45) "the 'common-law right of privacy' does *not* extend to the release of home 'addresses of public employees.'" But "both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person," as the Supreme Court has recognized. *RCFP*, 489 U.S. at 763; *FLRA*, 510 U.S. at 500 ("We are reluctant to disparage the privacy of the home, which is accorded special consideration in our

[11] Even under Defendants' cases relying on a secrecy conception, an address cannot not qualify as a "public fact" if it is no longer in records "open to public inspection." *McNutt*, 538 P.2d at 808.

Constitution, laws, and traditions."). Defendants' own authority concedes that under the traditional conception of privacy as "the right to be let alone," the publication of a "residential address" ***does*** "qualify as an invasion of that person's privacy" if "it would bring persons to that address to molest and harass the occupant." P. Hassman, *Public Addresses as Well as Name of Person as Invasion of Privacy*, 84 A.L.R.3d 1159 § 1 (1978) (cited by Defendants at 45).

Defendants' cases wrongly assume that disclosing an address cannot violate privacy because "addresses are not ordinarily personal, intimate, or embarrassing pieces of information." *Tobin v. Mich. Civil. Serv. Comm'n*, 331 N.W.2d 184, 189 (Mich. 1982). But Daniel's Law does not target "embarrassment or reputational damage." *Ostergren*, 615 F.3d at 282. It exists to address "a very real threat to the officers' and their family members' personal security and bodily integrity, and possibly their lives." *Kallstrom*, 136 F.3d at 1064.[12]

[12] Even Defendants' cases relying on a secrecy conception only hold that disclosure of an address "*without more*, cannot be viewed as an invasion of privacy." *See McNutt*, 538 P.2d at 809; *Tobin*, 331 N.W.2d at 191 (same). And courts have recognized that disclosures of facts that expose others to threats can be actionable even under the "highly offensive" test. *E.g.*, *Capra v. Thoroughbred Racing Ass'n of N. Am., Inc.*, 787 F.2d 463, 464-65 (9th Cir. 1986); *Hyde v. City of Columbia*, 637 S.W.2d 251, 254 (Mo. Ct. App. 1982).

D. Defendants' Facial Challenge Fails Because Daniel's Law Does Not Regulate Speech on A Matter of Public Concern in Virtually Any Applications

Under the *Daily Mail* test, Defendants cannot show that Daniel's Law is facially unconstitutional, much less in a motion-to-dismiss posture. Because Defendants chose to facially challenge Daniel's Law, they have the burden to show that the statute "prohibits a substantial amount of protected speech relative to its plainly legitimate sweep." *United States v. Hansen*, 599 U.S. 762, 770 (2023). But under the *Daily Mail* test, showing that a statute is unconstitutional even in ***a particular application*** requires showing both (i) that the Defendant disclosed "'truthful information about a matter of public significance'" ***and*** (ii) that "imposing liability" on the Defendant would not "'further a state interest of the highest order.'" *Florida Star*, 491 U.S. at 536 (quoting *Daily Mail*, 443 U.S. at 103). When both of those conditions are met, the statute is unconstitutional as-applied to the disclosure of private information at issue. But in all other applications, the claimant's privacy interest outweighs the defendant's speech interests, and the defendants is not "entitled to 'special protection' under the First Amendment." *Snyder*, 562 U.S. at 458; *Gilbert v. Medical Economics Co.*, 665 F.2d 305, 308 (10th Cir. 1981) ("[D]issemination of non-newsworthy private facts is not protected.").

Thus, to establish that Daniel's Law is ***facially*** invalid under the *Daily Mail* test, Defendants need to show:

(i) Daniel's Law regulates disclosures on a matter of public concern in a substantial number of applications;

(ii) In those applications, Daniel's Law is unconstitutional, because imposing liability would not further a state interest of the highest order; and

(iii) The "number" of unconstitutional applications of Daniel's Law is "substantially disproportionate to the statute's lawful sweep."

Defendants' facial challenge fails at the first step of this inquiry. Defendants ***never argued*** that Daniel's Law regulates speech on a matter of public concern in a significant number of applications below. *See* ECF 27-33 at 31 n.25. Nor did they argue that the statute is unconstitutional in applications in which it regulates speech on a matter of public concern, or that the number of unconstitutional applications of the statute is "substantially disproportionate" to the statute's concededly lawful sweep. Thus, Defendants forfeited any challenge to the District Court's ruling that the statute does not regulate speech on a matter of public concern in most of its applications. *See Robinson v. First State Cmty. Action Agency*, 920 F.3d 182, 187 (3d Cir. 2019).

Even if the Court considers Defendants' arguments, it is obvious that Daniel's Law does not regulate speech on a matter of public concern in most of its applications. As Defendants' own cases recognize, disclosures of addresses and similar information only qualify as speech on a matter of public concern when the

use of that information is "integral to their message" on an issue of public significance. *Ostergren*, 615 F.3d at 271; *Publius v. Boyer-Vine*, 237 F.Supp.3d 997, 1016 (E.D. Cal. 2017) (blog protesting database listing addresses of gun owners by posting addresses of legislators who voted for the law). Outside of such rare cases, disclosures of such information typically "concern[] no public issue" and relate only to the "private" interests of those who wish to contact that person. *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 762 (1985); *Trans Union Corp. v. F.T.C.*, 267 F.3d 1138, 1140 (D.C. Cir. 2001) ("[N]ames, addresses, and financial circumstances" were "speech of purely private concern.").

At minimum, Defendants could not establish that a substantial number of disclosures regulated by Daniel's Law concern any matter of public significance on a motion to dismiss. Defendants note that when the tiers of scrutiny apply, a statute that "fails the relevant constitutional test (such as strict scrutiny…or reasonableness review) can no longer be constitutionally applied to anyone"—thus eliminating the need to prove invalidity on an application-by-application basis. *Bruni v. City of Pittsburgh*, 824 F.3d 353, 363 (3d Cir. 2016). But this logic does not apply under the *Daily Mail* test, because its first step requires a threshold inquiry into whether the particular defendant disclosed truthful information on a matter of public concern. As the Supreme Court has explained, "[d]eciding whether speech is of public or private concern" ordinarily requires examination of "the content, form, and context of that

speech, as revealed by the whole record," including "what was said, where it was said, and how it was said." *Snyder*, 562 U.S. at 453-54.

Defendants argue (at 49-50) that addresses and phone numbers contained in public records "*necessarily* are matters of public concern." But whether an address is contained in a public record has nothing to do with whether a ***disclosure*** of that address concerns a "matter of political, social, or other concern." *Snyder*, 562 U.S. at 453.[13] And regardless of whether "[h]istorically, people's addresses and phone numbers have been publicly available," as Defendants claim (at 50), historical accessibility has no bearing on whether a disclosure regulated by the statute addresses "a subject of general interest and value and concern to the public at the time of publication." *Roe*, 543 U.S. at 83-84.[14]

Similarly, even if disclosing a covered person's address might, hypothetically, be "necessary for public oversight'" in some cases, as Defendants suggest (at 50-51), that would at most show ***some*** disclosures regulated by Daniel's Law involve

[13] Neither *Florida Star* nor *Cox Broadcasting* suggest everything in a public record is automatically of public concern. *Cox* noted public records "are of interest to those concerned with the administration of government," but the Court was discussing reporting "by the media," 420 U.S. at 495, and concluded three pages earlier that the news at issue was "of legitimate concern." *Id.* at 492.

[14] Defendants ignore that "public availability" meant something very different before modern computerized public-record keeping and data mining. And "[b]efore the mid-nineteenth century, few public records were collected, and most of them were kept at a very local level." D. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 Minn. L. Rev. 1137, 1142 (2002).

speech of public concern—not that ***every*** such disclosure does. *But see Kratovil v. City of New Brunswick*, 2024 WL 1826867, at *5 (N.J. App. 2024) ("[T]he publication of the town where Caputo lived was a matter of public concern, but Caputo's specific street address was not."). But the prospect of a handful of ***potential*** as-applied challenges cannot establish that the "number" of unconstitutional applications of the statute is "substantially disproportionate" to its concededly "lawful sweep." *Hansen*, 599 U.S. at 770. And "[i]n the absence of a lopsided ratio, courts must handle unconstitutional applications as they usually do—case-by-case." *Id*.

In sum, because Daniel's Law does not regulate speech on matters of public concern in the bulk of its applications, the statute clearly withstands facial scrutiny. In all applications in which the statute does not regulate speech on a matter of public concern, the First Amendment does not prohibit courts from imposing liability. When the statute does regulate speech on a matter of public concern, defendants in those cases may challenge the statute on an as-applied basis.

II. At Most, Intermediate Scrutiny Applies To Daniel's Law

If the Court believes *Daily Mail*'s test does not apply, it should analyze Daniel's Law under intermediate scrutiny for three independent reasons: (i) Daniel's Law is not content based; (ii) it is a narrower version of a privacy tort with a

longstanding coexistence with the First Amendment; and (iii) it poses no risk of viewpoint discrimination.

A. Daniel's Law Is Not Content Based

Below, the District Court rejected Plaintiffs' argument that Daniel's Law is not content based. JA104. If the Court reaches this issue, it should conclude that the District Court erred on this point and apply intermediate scrutiny. A regulation is content based if it "targets speech based on its communicative content—that is, if it applies to particular speech because of the topic discussed or the idea or message expressed." *City of Austin v. Reagan Nat'l Advert. of Austin, LLC*, 596 U.S. 61, 69 (2022). "Content neutral laws, on the other hand," regulate "based on some other neutral characteristic of the speech." *Mazo v. New Jersey Sec'y of State*, 54 F.4th 124, 148 (3d Cir. 2022). Thus, a law can be content-neutral even though applying it "may require some evaluation of the speech." *City of Austin*, 596 U.S. at 72. "A regulation may remain content neutral despite touching on content to distinguish between classes or types of speech…so long as it does not discriminate on the basis of viewpoint or restrict discussion of an entire topic." *Schmidt*, 125 F.4th at 950. If the law "is agnostic as to content" and "requires an examination of speech only in service of drawing neutral lines," it is content-neutral. *Mazo*, 54 F.4th at 149.

The addresses and phone numbers regulated by the statute do not in themselves qualify as "content," and the statute does not "target" that data by

reference to any message of the speaker. Data or symbolic representations are not the same thing as the "communicative content" protected by the First Amendment. The "communicative content" of a speech act is the "topic discussed or an idea or message expressed," but in itself, an address or phone number is not a "topic," "idea," or "message." *City of Austin*, 596 U.S. at 69. Moreover, Daniel's Law prohibits disclosure of a covered person's information only when the defendant received a nondisclosure request. Thus, the statute is "agnostic to the dissemination of" contact information when no request for non-disclosure has been made, and makes no attempt to target communication regarding a covered person's contact information absent such a request. *Dahlstrom v. Sun-Times Media, LLC*, 777 F.3d 947, 949 (7th Cir. 2015). The speaker's "substantive message itself is irrelevant to the application" of the statute. *City of Austin*, 596 U.S. at 71. The statute at most "implicate[s] the content of speech…in a manner that [is] neutral with respect to the message that individual speakers express." *Schmidt*, 125 F.4th at 949.

B. Disclosure Torts Have Long Coexisted With The First Amendment

Daniel's Law also evades "heightened scrutiny" because it belongs to a family of common-law and statutory torts of "longstanding coexistence with the First Amendment." *Vidal*, 602 U.S. at 300. Daniel's Law is a more narrowly targeted version of the common-law "cause of action for invasion of privacy through public disclosure," which typically "imposes sanctions on…the content of a publication."

Cox Broadcasting, 420 U.S. at 495; *cf. Vidal*, 602 U.S. at 300 (refusing to apply strict scrutiny to a "uniquely content based" area of law). Such torts have coexisted with the First Amendment since they were developed more than a century ago—and even then, courts affirmed that "[t]he right to speak and the right to privacy have been coexistent." *Pavesich*, 50 S.E. at 73. Daniel's Law does not imperil First Amendment interests any more than common-law disclosure, misappropriation, and intrusion torts—it restricts far less speech because it is narrowly restricted to two bits of data that have virtually no relevance to any viewpoint or matter of public concern.

C. Daniel's Law Creates No Risk of Viewpoint Discrimination

Finally, any risk of viewpoint discrimination associated with Daniel's Law is trivial, so "intermediate scrutiny" applies to the statute even "without any reliance on history." *VoteAmerica*, 121 F.4th at 849. "[T]he rationale of the general prohibition" on "content discrimination" is that it "raises the specter that the Government may effectively drive certain ideas or viewpoints from the marketplace." *Davenport v. Wash. Educ. Ass'n*, 551 U.S. 177, 188 (2007). "But the Supreme Court has 'identified numerous situations in which" the risk of viewpoint discrimination "'is inconsequential, so that strict scrutiny is unwarranted.'" *VoteAmerica*, 121 F.4th at 848 (quoting *Davenport*, 551 U.S. at 188); *see also Vidal*, 602 U.S. at 311 (Kavanaugh, J., concurring) ("[A] viewpoint-neutral, content-based"

restriction "might well be constitutional even absent such a historical pedigree."); *id.* at 312-13 (Barrett, J., concurring) (same).

Daniel's Law poses no risk of viewpoint discrimination, so there is no justification for applying strict scrutiny here. The statute does not target "the specific motivating ideology or the opinion or perspective of the speaker" or threaten to "discriminate based on viewpoint in its practical operation." *Vidal*, 602 U.S. at 294. It regulates two—and only two—bits of information, both of which are irrelevant to the expression of any viewpoint. And "where matters of purely private significance are at issue, First Amendment protections are often less rigorous." *Dun & Bradstreet,* 472 U.S. at 762; *Trans Union*, 267 F.3d at 1141 (applying intermediate scrutiny applied to marketing lists containing "names" and "addresses").[15]

Other features of the law compel the same conclusion. As in *Davenport*, the Legislature was "acting in a capacity other than as regulator" when it enacted Daniel's Law, because the statute creates a private cause of action rather than a state-enforced mandate. 551 U.S. at 188 (refusing to apply strict scrutiny to statute "requiring affirmative consent only for election-related expenditures"). Thus, any "risk" Daniel's Law "will impermissibly interfere with the marketplace of ideas" is

[15] *Sorrell v. IMS Health, Inc.*, 564 U.S. (2011), is not to the contrary. As this Court explained, "it is not even clear that the Court applied strict scrutiny" in *Sorrell* "even though the statute there was neither viewpoint neutral nor speaker neutral." *Greater Philadelphia Chamber of Commerce v. City of Philadelphia*, 949 F.3d 116, 140 (3d Cir. 2020).

"attenuated." *Id.* Moreover, as in *Davenport*, the statute imposes a "restriction on [a] state-bestowed entitlement" to remedy a "state-created harm" caused by unregulated access to data in government records. *Id.* at 189. And finally, preventing dissemination of the protected information of covered persons protects the "social interest in order," which "outweighs the negligible contribution" made "to the marketplace of ideas." *Id.* at 188; *People v. Austin*, 155 N.E.3d 439, 459 (Ill. 2019) (intermediate scrutiny applied to revenge-pornography statute that had no "potential for censorship").

III. Daniel's Law Satisfies Any Standard Of Scrutiny

If the Court examines whether Daniel's Law is narrowly tailored, it should affirm the District Court's ruling regardless of which standard of scrutiny applies. Strict scrutiny requires statutes to "be narrowly tailored" to serve a compelling state interest, "not that it be perfectly tailored." *Williams-Yulee v. Florida Bar*, 575 U.S. 433, 454 (2015). Under intermediate scrutiny, a regulation must "directly advance[]" a "substantial" government interest but "need not be the least restrictive means," and only a "reasonable fit between the legislature's ends and the means chosen" is necessary. *Greater Philadelphia*, 949 F.3d at 138.

Here, Defendants concede (at 25) that "the safety interest underlying Daniel's Law is compelling." As explained, *supra* 23-27, the statute also "protect[s]

individual privacy" which "certainly constitute[s] 'a state interest of the highest order.'" *Ostergren*, 615 F.3d at 280 (quoting *Daily Mail*, 443 U.S. at 103).

A. Daniel's Law Is Not Overinclusive

Defendants claim Daniel's Law is overinclusive, but the handful of purported problems with the statute's tailoring they identify do not show a deficiency even under strict scrutiny, let alone intermediate scrutiny.

1. Definition of "Disclose"

Defendants argue (at 26-27) that Daniel's Law is overinclusive because its definition of "disclose" prohibits disclosures that supposedly have "no apparent nexus" with the State's interest. They suggest the Legislature should have narrowed the definition to publications made "available to the general public," Md. Code Ann., Cts & Jud. Proc. § 3-2301(f), to information "publicly posted," Federal Daniel Anderl Judicial Security and Privacy Act of 2022, Pub. L. No. 116-263, §§ 5933, 5934, 136 Stat. 2395, 3460-65 (2022), or to disclosures only by a narrowly defined set of "data brokers". *Id.*

In principle, all of these alternatives are permissible because the protected information of covered persons virtually never implicates any matter of public concern. But if heightened scrutiny applies here, as Defendants contend, restricting the scope of "disclosure" to publications or creating speaker-based carveouts might create the same underinclusiveness problem that the Supreme Court identified with

the statute at issue in *Florida Star*: adopting a "selective ban on publication by mass media" that fails to account for "alternative dissemination." 491 U.S. at 540-41 (emphasis added). By defining "disclose" to cover essentially all disclosures likely to expose protected information, Daniel's Law incorporates precisely the "more careful ***and inclusive*** precautions against alternative dissemination" the Court advised. 491 U.S. at 540-41 (emphasis added).

Defendants' suggestion that the statute somehow precludes transactions that "are necessary for modern society to function" ignores that a duty not to disclose arises if and only if a covered person has sent a nondisclosure request to a business and does not subsequently authorize disclosure to facilitate a desired transaction. Thus, "*transferring*" a covered person's name and address to a vendor for shipping a product will almost never trigger a violation of the statute, because the covered person will have authorized the transaction and disclosure. Similarly, a business delivery or giving information to another business for a credit check or to prevent bank fraud is not violative of the law, unless the covered person has sent a nondisclosure request and the business originating the transaction does not subsequently obtain an appropriate authorization from that covered person.

Defendants provide a list of hypothetical disclosures that they claim are unlikely to endanger covered persons. But their examples reflect a dangerous misunderstanding of how public servants have been targeted in the past. Most

obviously, an attorney targeted Judge Salas and murdered her son. If "*providing*" an address to a law firm were exempted from the statute, it could not even have prevented the very murder that led to its enactment. Such an assailant could obtain a judge or other covered person's information from a data broker under the guise of that broker "*providing*" information to facilitate service of process. *Cf. Kallstrom*, 136 F.3d at 1064 (disclosure to "defense counsel" created "a serious risk to the personal safety of the plaintiffs" and "their family members").

Exempting business-to-business disclosures from the statute would create a limitless backdoor and negate the entire purpose of Daniel's Law. Defendants claim that business-to-business disclosures have "no apparent nexus" to an individual's safety concerns, perhaps unaware that the gunman who killed Maryland Circuit Court Judge Andrew Wilkinson at his home in October 2023 was the owner of a failing digital-marketing business who could have easily exploited such an exemption. In these cases, Plaintiff Jane Doe-1 (a law-enforcement officer) and her children were targeted at home by a criminal organization who obtained her address from a private investigation firm with access to business-to-business data brokers. JA487.

Moreover, even when both parties to a business-to-business disclosure have legitimate purposes, such disclosures create an obvious risk of "unauthorized subsequent disclosures." *Westinghouse*, 638 F.2d at 580. When a business transfers

an address to another business, the transferor has no control over whether the transferee (or others to whom the transferee sells it) will post that information online. Widespread dissemination among businesses also increases the risk that hackers or other illicit actors can breach a database and sell the contents. "When that information is made available for download on the Dark Web—a platform that exists primarily to facilitate illegal activity—the risk that a criminal will access it and use it for a nefarious purpose is particularly acute." *Clemens v. ExecuPharm, Inc.*, 48 F.4th 146, 159 (3d Cir. 2022) ("Victims of a data breach must live with the perpetual, well-founded fear and risk that hackers will misuse their data.").

Defendants' claim (at 37) that the statute's definition of "disclose" "may even cover purely internal business activities" and bar "internal corporate communications" is nonsensical: a company is not ***disclosing*** **or** *making available* anything when information is merely internally available. Recipients of nondisclosure requests must engage in internal communications and maintain internal records to comply with the statute. Defendants are wrong to take issue (at 37) with "disclosure" including protected information available within a searchable database (which is itself then made available to third parties) "regardless of whether a search is actually performed." Defendants' objection overlooks the purpose of Daniel's Law: to require proactive compliance with nondisclosure requests *before* a search for the covered person is performed, not merely to compensate victims after

their information has been retrieved and weaponized against them. As the District Court noted, waiting for 'true threats' as Defendants' propose would be "analogous to closing the barn door after the horse has left." JA114. Here, of course, the risks and consequences are much more severe than a lost horse.

2. Public Records

Defendants' argument (at 28-29) that Daniel's Law is overinclusive because it prevents defendants from disclosing addresses that remain available in public records grossly overstates the extent to which Daniel's Law exempts any public records from redaction through OIP's process. But Defendants' argument at most shows the statute is ***under*inclusive**, not ***over*inclusive**. And "underinclusiveness is only important…if it raises serious doubts about whether the government is in fact pursuing the interest it invokes, rather than disfavoring a particular speaker or viewpoint." *Greater Philadelphia*, 949 F.3d at 156.

Contrary to what Defendants argue, the very existence of OIP proves that the law is a comprehensive statutory regime designed to remove address and telephone information from state and business records—with OIP's process enabling covered persons to redact their addresses from records that are frequently mined for data. Defendants do not mention any purported loopholes in the redaction scheme for phone numbers, because there are none—the limited records containing personal phone numbers cannot be disclosed by New Jersey public agencies. *See* N.J.S.A.

47:1A-1.1 (noting that a portion of any document containing any telephone number is deemed confidential and excluded from the definition of a "Government Record"). Thus, from the outset, Defendants effectively concede that the scheme is appropriately tailored as to phone numbers. And as applied to addresses, the regulatory scheme is far more comprehensive than the in-person access system Defendants' case suggests would be "narrowly tailored to protect[] individual privacy." *Ostergren*, 615 F.3d at 285-86 (recognizing a "critical difference between original land records available from courthouses and digital land records").

The statute enables covered persons to redact their address from virtually any property record "recorded and indexed by a county recording officer" or "by the Division of Taxation, a county board of taxation, a county tax administrator, or a county or municipal tax assessor." *Id.* 47:1B-3(a)(2). By the terms of the statute, any "document affecting the title to real property" is subject to redaction "[o]ther than as provided in subparagraphs (d) and (e) of paragraph (4), N.J.S.A. 47:1B-3(a)(4)(d) and (e). *Id.* 47:1B-3(a)(2). Thus, unless a "document affecting the title to real property" falls under one of the exceptions in subparagraph (d) or (e), it cannot be viewed unredacted by any member of the public. The agency responsible for redaction "may instead or in addition" to redacting the covered person's address, redact "the names or other information" of the covered person," and licensed real-estate professionals are granted unredacted access "when requested" in "the ordinary

course of business." *Id.* 47:1B-3(a)(2). But such disclosures present limited risks to covered persons and are essential to the operation of New Jersey's real-estate market.

The exceptions in subparagraphs (d) and (e) do not allow the public to access the address of a covered person. Defendants focus on subparagraph (d), which exempts "records evidencing any lien, judgment, or other encumbrance on real or other property," but this exemption creates only a limited carve-out to the statute's general requirement that public agencies redact names or addresses from all "document[s] affecting the title to real property." N.J.S.A. 46.26A-2 defines "document[s] affecting title to real property" to include seventeen categories of documents. Of those seventeen categories, only "liens or encumbrances" and "certified copies of judgments, decrees and orders of courts of record" are referenced by N.J.S.A. 47:1B-3(a)(4)(d). No other category of "document affecting the title to real property" listed in 46:26A-2 is accessible to the public. This includes deeds, leases, mortgages, "any other document that affects title to any interest in real property in any way," and "any other document relating to real property that is directed to be recorded by any statute or court order." N.J.S.A. 46:26A-2.

Subparagraph (e) exempts "assessment lists" subject to inspection "in person." N.J.S.A. 47:1B-3(a)(4)(e). But the record custodian "shall make every reasonable effort to hide such address when allowing an individual without authority to view such address as unredacted to view the record." *Id.* 47:1B-3(a)(6). And as

the Supreme Court has held, there is "a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information." *RCFP.,* 489 U.S. at 764; *Ostergren*, 615 F.3d at 285-86. Thus, at most, covered persons whose addresses are listed in a recorded lien, encumbrance, or certified judgment may not be able to redact their address from every publicly available record under N.J.S.A. 47:1B-3(a)(4)(d). All other covered persons can redact their information from State and local property records.

Nor does Daniel's Law prevent covered persons from redacting protected information from voter records. The statute provides that "[c]opies of voter registration files . . . be provided as redacted" except to a handful of narrowly defined categories of individuals, such as county or municipal party chairs, candidates, vendors and contractors "carrying out a function of a county or of the State concerning the administration or conduct of elections," and "upon the order of a judge" upon "a finding that the unredacted copy is necessary to determine the merits of a petition." N.J.S.A. 47:1B-3(a)(1)(a)-(e).

Even if a particular covered person's address remains available in a record accessible to the general public, Defendants are wrong to claim (at 28) that the Supreme Court "has held that the government is constitutionally foreclosed from imposing liability for publishing information" as a categorical rule. For one, all of

the Supreme Court's cases on this issue presupposed that the speech at issue was on a matter of public concern. Beyond that, the Court's holding in those cases was premised on a "different conception[] of privacy—one focused upon secrecy and incompatible with any disclosure," rather than one "focused upon control and consistent with limited disclosure." *Ostergren*, 615 F.3d at 285 (distinguishing *Cox Broadcasting* and *Florida Star* "where the government did not have to search for the sensitive information needing redaction"). When a privacy interest is founded on secrecy, there is little reason to impose liability for disclosures that have already occurred. But when, as here, a privacy interest is based on a need for control, restrictions on re-disclosure are "narrowly tailored" to "protect individual privacy" so long as they eliminate easy public access to unredacted records. *Id.* at 286-87.

3. Verification

Next, Defendants claim (at 29-30) Daniel's Law is overinclusive because it does not require covered persons to "verify" they are covered by the statute in nondisclosure requests. But verification has nothing to do with whether the statute is overinclusive—and conveniently for Defendants, requiring verification would make it burdensome for covered persons to enforce their rights. Ordinarily, a plaintiff does not need the State's approval to send a demand letter or file a lawsuit, and Defendants cannot point to any First Amendment principle that would justify imposing such an extraordinary requirement. And if someone who is not a covered

person brings a suit under the statute in bad faith, Defendants can use the traditional tools to combat bad-faith litigation, such as a malicious-prosecution action or filing a bar complaint against the attorney who brought the suit.[16]

4. Assignment and Penalties

Defendants' next complaints (at 30-31) are directed at the assignment and liquidated-damages provisions of the statute, but neither provision even restricts speech. As this Court has explained, "a penalty for noncompliance with a restriction on speech is not equivalent to a restriction on speech," and "the kind of penalty" that the Legislature "chose is not a basis to decide that the [s]tatute could be less restrictive." *Free Speech Coal., Inc. v. Attorney General*, 974 F.3d 408, 426 (3d Cir. 2020). Similarly, the assignment provision does nothing to restrict speech, because it has no bearing on what speech is or is not allowed.

Both provisions advance the State's concededly compelling interest in preventing widespread dissemination of the protected information of covered persons. Assignment guarantees by statute the right of covered persons to seek assistance with the enforcement of their rights from an assignee who is well-positioned to identify, monitor, and bring suit against violators. Likewise, default damages are necessary to set a baseline value for compensatory damages and to deter

[16] Defendants are simply wrong when they claim that verification existed in the prior version of Daniel's Law. OIP has never provided a verification mechanism for use in confirming a covered person's status.

violations of the statute. Without the threat of monetary liability, defendants would have virtually no incentive to comply with the law. Most covered persons would not be able to retain counsel to litigate low-value claims, and "peoplefinder" websites and other data brokers could ignore Daniel's Law with impunity.

5. Unpublished Telephone Numbers

Finally, Defendants argue that Daniel's law is overinclusive because it does not define "unpublished telephone number," but the concept is well understood: it means a phone number that is not currently listed in a local telephone directory. *Cf.* Cal. Pub. Util. Code § 2891.1(h) (defining "unpublished" numbers as those that the assigned subscriber requested to have kept "in confidence"). Telephone directories may not be ubiquitous anymore, but they still exist.

B. Daniel's Law Is Not Underinclusive

Next, Defendants identify three supposed underinclusiveness problems with Daniel's Law (at 32-36), but they are nonstarters. First**,** Defendants reiterate their argument (at 32-33) about public records, but are wrong for the reasons given above.

Second, Defendants argue that the statute should have required covered persons to complete OIP's process before they could exercise their right to request nondisclosure from private entities. But this argument does not even address phone numbers, and there is no reason why the statute's aims mandate that covered persons take advantage of OIP's redaction process as a condition of exercising their rights

against private entities. For some covered persons, sufficient privacy and safety can be attained through redaction from "peoplefinder" websites and data clearinghouses, particularly for the subset of covered persons whose threats come predominantly from individuals who rely on easier ways to harass or threaten them. Such covered persons may have good reason to forego OIP's process, which requires one to "affirm in writing" that "certain rights, duties, and obligations are affected as a result of the request." N.J.S.A. 47:1B-2d(1)-(6) (enumerating potential consequences from eligibility to hold office to "recordation of a judgment, lien, or other encumbrance" and notice of "class action[s]").

Third, Defendants posit that Daniel's Law is underinclusive because the Legislature did not absurdly prohibit covered persons from disclosing their ***own*** protected information. But as Defendants' own examples illustrate, covered persons ***must*** be able to voluntarily disclose their own address or phone number to engage in a variety of transactions, from authorizing a credit check to ordering a product for delivery at their home address. The Legislature's choice in "regulatory scheme" to "allow [a covered person] to remain in control of that information and…decide whether s/he wants to disclose it" was entirely justified. *Greater Philadelphia*, 949 F.3d at 156.

C. Defendants' Purportedly Less-Restrictive Alternatives Do Not Advance The State's Interests

Defendants identify five supposed "less-restrictive alternatives," but four of them are reiterations of their attacks on the definition of "disclose," the assignment and damages provisions, and the absence of a verification requirement. As explained, narrowing the definition of "disclose" to publication could introduce the selective ban on mass dissemination condemned in *Florida Star*, and the other alternatives have nothing to do with speech restriction. Defendants assert (at 36-37) that Plaintiffs have a "burden" to prove these alternatives are less effective, but "simple common sense" shows they are. *Greater Philadelphia*, 949 F.3d at 143 (common sense can justify restrictions even "*applying strict scrutiny*"). Their only other alternative proposes to (at 38) exempt information "the government or covered persons themselves make public." But it would have been irrational for the Legislature to make a covered person's protected information fair game for disclosure and re-disclosure simply because it appears in a now-unredacted public record or because the covered person disclosed it publicly in some particular format on some particular occasion. With this approach, the law never would have gotten off the ground, because the point of the statute is to eliminate contact data from pre-existing widespread availability that proved incompatible with the safety and privacy of covered persons.

D. Daniel's Law Requires Proof of Ordinary Negligence

Finally, Defendants argue that the District Court should have interpreted Daniel's Law as a strict-liability statute and held it unconstitutional on that basis. But the District Court had no reason to *affirmatively interpret* a statute that is *silent* on the standard of care as a strict-liability statute *in order to create a constitutional problem with it*, as Defendants propose. Defendants' argument inverts the usual rule of statutory interpretation, in which courts "assume that the Legislature would want [the court] to construe the statute in a way that ***conforms*** to the Constitution." *State v. Pomianek*, 110 A.3d 841, 857 (N.J. 2015) (emphasis added). "[W]hen evaluating a constitutional challenge to a statute," New Jersey courts "presume that the [L]egislature acted with existing constitutional law in mind and intended the [statute] to function in a constitutional manner." *Gallenthin Realty Dev., Inc. v. Borough of Paulsboro*, 924 A.2d 447, 457 (N.J. 2007). Thus, courts must "construe the statute as to render it constitutional if it is reasonably susceptible to such interpretation." *Id.*

Here, the District Court's interpretation was more than reasonable: the court was clearly correct that Daniel's Law imposes liability only if a defendant is unreasonable in disclosing or otherwise making available a covered person's protected information after the statutory deadline had expired. JA120. The text of Daniel's Law nowhere suggests that defendants are strictly liable for "disclosing, re-disclosing, or otherwise making available" the protected information of a covered

person even if they made a reasonably diligent effort to comply with their Daniel's Law obligations. N.J.S.A. 56:8-166.1a(1). And New Jersey courts will not read a strict-liability standard into a statute "[i]n the absence of any language expressly" requiring one. *Mascola v. Mascola*, 401 A.2d 1114, 1118 (N.J. Supr. App. Div. 1979); *Goldhagen v. Pasmowitz*, 255 A.3d 1191, 1198–99 (N.J. 2021). Under New Jersey law, statutes "in derogation of the common law" are "strictly construed," *Marshall v. Klebanov*, 902 A.2d 873, 881 (N.J. 2006), and negligence *per se* standards are highly disfavored. *Labega v. Joshi*, 270 A.3d 378, 388-89, 490 n. 6 (N.J. Supr. App. Div. 2022) (New Jersey is "among the 'small minority'" of states that have rejected negligence *per se*).

Instead, when "[a] literal reading" of a statute "does not 4ide a definitive answer," New Jersey courts rely on "common law analogues" to arrive at the correct "interpretation of the statute." *Evans-Aristocrat Indus., Inc. v. Newark*, 380 A.2d 268, 272-73 (N.J. 1977); *G.D. v. Kenny*, 15 A.3d 300, 314 (N.J. 2011) (interpreting statute "[i]n light of common-law and constitutional principles respecting free speech"). The most obvious analogue of Daniel's Law, the "the invasion of privacy by unreasonable publication of private facts" tort—operates with a negligence standard that requires actual or constructive knowledge that the fact disclosed was offensive or would otherwise interfere with the plaintiff's privacy interests. *Romaine*

v. Kallinger, 537 A.2d 284, 297-98 (N.J. 1988).[17] Daniel's Law is also analogous to two other privacy torts recognized in New Jersey, neither of which imposes liability on a no-fault standard: (i) intrusion upon seclusion; and (ii) misappropriation of name and likeness. *See Bisbee v. John C. Conover Agency, Inc.*, 452 A.2d 689 (N.J. 1982). The District Court had no reason to impose a strict-liability standard on Daniel's Law either."[18]

Defendants claim (at 60) that "a speech restriction imposing liability must include a robust 'scienter requirement.'" (quoting *Florida Star*, 491 U.S. at 539). But *Florida Star* did not purport to require a standard higher than "ordinary negligence." *Id.* at 539. *Counterman v. Colorado* simply reiterated that the Supreme Court has "adopted a recklessness rule" in its "defamation decisions." 600 U.S. 66, 81 (2023), But the Supreme Court has never imposed an "actual malice" standard on any privacy torts other than the "false light" tort, which, like defamation, involves misrepresentation. *Time*, 385 U.S. at 388. And in the defamation context, the First

[17] *See, e.g.*, *Steinbuch v. Hachette Book Grp.*, 2009 WL 963588, at *3 (E.D. Ark. 2009).

[18] Defendants' cases involved obvious re-writes of statutes, not interpreting a statute silent on the issue based on common-law principles. *See Pomianeki*, 110 A.3d at 90 (Lower court "erred by rewriting the statute to impose a mens rea element almost identical to the one in [another] subsection."); *Usachenok v. Department of the Treasury*, 313 A.3d 53, 64 (N.J. 2024) (adding clause indicating compliance "is not mandatory" would "extend beyond the limits of judicial surgery").

Amendment does not require "a showing of 'actual malice'" when "statements do not involve matters of public concern," as here. *Dun & Bradstreet*, 472 U.S. at 763.

Finally, the statute's notification requirement ensures anyone who receives such a notification will know, or have strong reason to know, that disclosing or re-disclosing the protected information would violate the rights of that covered person. And because receipt of a nondisclosure request is a prerequisite to liability under the statute, Daniel's Law inherently requires plaintiffs to "prove, as an element of the cause of action, that the defendant had actual or constructive knowledge" their conduct would violate the rights of a covered person. *Troupe v. Bulington Coat Factory Warehouse Corp.*, 129 A.3d 1111, 1114 (N.J. Supr. App. Div. 2016).[19] That level of fault is more than sufficient under the First Amendment.

CONCLUSION

For these reasons, the Court should affirm denial of Defendants' Motion to Dismiss.

[19] Defendants note (at 57-58) that an earlier iteration of Daniel's Law imposed damages only if "a reasonable person would believe that providing…information would expose another to harassment or risk of harm to life or property." (quoting N.J. Sess. Law Serv. Ch. 125, § 6). In removing this language, the Legislature only eliminated the requirement of negligent indifference to the risk that a covered person would be ***harmed by disclosure***, which says nothing about whether a defendant exhibit negligent indifference to a risk that disclosing a covered person's protected information will violate their rights.

Respectfully submitted,

Dated: May 12, 2025

PEM LAW LLP

By: */s/Rajiv D. Parikh*
Rajiv D. Parikh, Esq.
(NJ Bar ID # 032462005)
Kathleen Barnett Einhorn, Esq.
Jessica A. Merejo, Esq.
One Boland Drive, Suite 101
West Orange, New Jersey 07052
Telephone: (973) 577-5500
Emails: rparikh@pemlawfirm.com
keinhorn@pemlawfirm.com
jmerejo@pemlawfirm.com

BOIES SCHILLER FLEXNER LLP

/s/Eric M. Palmer
Eric M. Palmer, Esq.
(FL Bar ID # 1050210)
401 E. Las Olas Blvd., Suite 1200
Fort Lauderdale, Florida 33301
Telephone: (954) 377-4250
Email: epalmer@bsfllp.com

David Boies, Esq.
55 Hudson Yards, 20th Floor
New York, New York 10001
Telephone: (919) 749-8200
Email: dboies@bsfllp.com

Mark C. Mao, Esq.
44 Montgomery Street, 41st Floor
San Francisco, California 94104
Telephone: (415) 293-6800
Email: mmao@bsfllp.com

Adam R. Shaw, Esq.
30 South Pearl Street, 12th Floor
Albany, New York 12207
Telephone: (518) 434-0600
Email: ashaw@bsfllp.com

MORGAN & MORGAN, P.A.
Ryan J. McGee, Esq.
John A. Yanchunis, Esq.
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Emails: rmcgee@forthepeople.com
jyanchunis@forthepeople.com

BIRD MARELLA RHOW LINCENBERG DROOKS NESSIM LLP
Ekwan E. Rhow, Esq.
Elliot C. Harvey Schatmeier, Esq.
Bill L. Clawges, Esq.
1875 Century Park East, 23rd Fl
Los Angeles, California 90067
Telephone: (310) 201-2100
Emails: erhow@birdmarella.com
ehs@birdmarella.com
bclawges@birdmarella.com

Attorneys for Appellees

CERTIFICATE OF COMPLIANCE

Pursuant to Rule 32(g) of the Federal Rules of Appellate Procedure, and Local Appellate Rules 28.3, 31.1, and 46.1, I hereby certify that:

1. This document complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B), because, according to the word count of the word-processing system used to prepare this document, the relevant portion of the document contains 12,963 words;

2. This document complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Office Word 365 in 14-point Times New Roman font;

3. The text of electronic Brief and the text of any paper copies to be filed with the Clerk are identical; and

4. The PDF file of this response has undergone a virus check using Huntress, Version 0.14.22 (last updated 04/22/2025), and no virus was detected.

5. I certify pursuant to Third Circuit Local Appellate Rules 28.3(d) and 46.1(e) that I am a member of good standing of the Bar of this Court.

Dated: May 12, 2025

/s/Rajiv D. Parikh
Rajiv D. Parikh

/s/Eric M. Palmer
Eric M. Palmer, Esq.

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Third Circuit by using the appellate CM/ECF system on May 12, 2025. Participants in the case are registered CM/ECF users, and service will be accomplished by the appellate CM/ECF system.

Dated: May 12, 2025

/s/Rajiv D. Parikh
Rajiv D. Parikh

/s/Eric M. Palmer
Eric M. Palmer